OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Intelligence Integration into Resource Process and Acquisition Lifecycle

Intelligence Strategy, Programs and Resources

Briefing to DAU
April 7, 2015

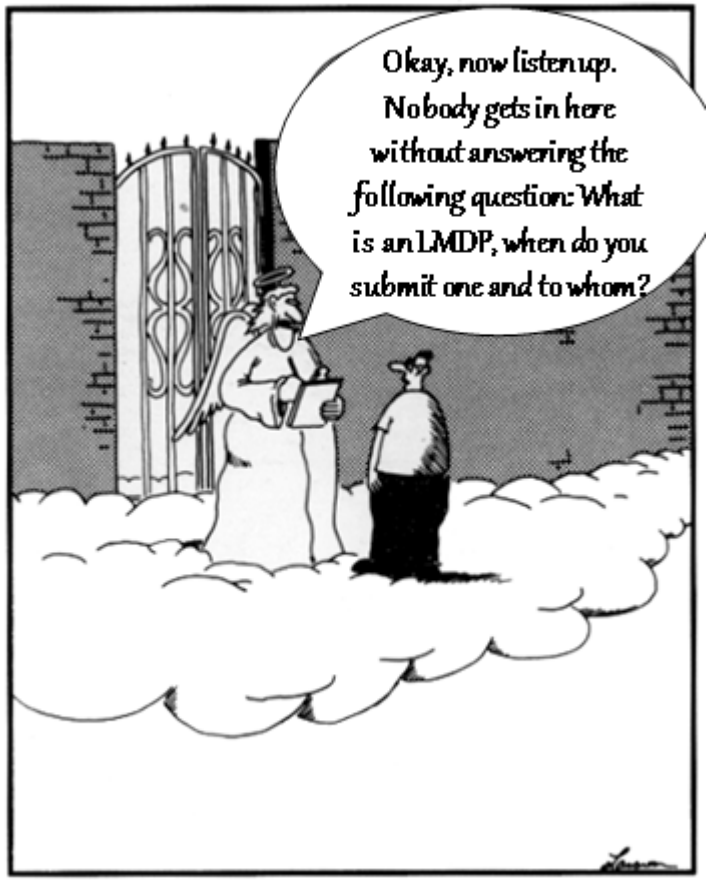
OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Improving Intelligence Integration in Acquisition

Intelligence Strategy, Programs and Resources

Agenda:

- BLUF
- Why do you care?
- What is the IC?
- How do you make it work for
- What's changed/changing?
- Way Ahead


Okay, now listen up. Nobody gets in here without answering the following question: What is an LMDP, when do you submit one and to whom?

Program Manager's nightmare

Improving Intelligence Integration in Acquisition

Bottom Line Up Front:

- **"Houston, we have a problem"**
  - **JSF brought threat and IMD issue to forefront**
- **The light you see is not the end of the tunnel —its a train coming**
  - **Next generation weapons reliance on up to date threat and intelligence supportability is increasing**
  - **Resources anticipated to be flat or declining**
- **Definition of Insanity—Doing the same thing and expecting different results**
- **USD(I), AT&L, DIA, Services, and ODNI working to implement solutions this year**

DONE RIGHT: IMPROVES COMBAT CAPABILITIES, EFFICIENCIES, SAVINGS

Why Do You Care as a Program Manager?

- **AT&L Vision:** Drive the capability to defeat any adversary on any battlefield
- **Your Challenge:** Deliver those capabilities on cost, schedule, and performance, often for long term programs in a rapidly changing environment
- **JSF Case Study:** Threat and IMD

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Improving Intelligence Integration in Acquisition

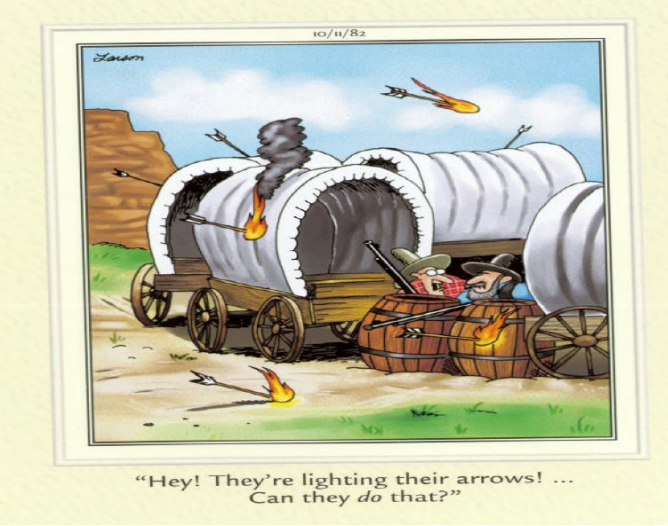
Intelligence Strategy, Programs and Resources

Taking the mystery out of Intelligence:

- **Like the Acquisition Community, the IC is big and complex**

- **Operates as a Federation in addressing your needs:**
  - **DIA manages the Federated Enterprise**
  - **Your Service Intelligence Chief is y**

- **Rules of Thumb in dealing with**
  - **Resource Constrained**
  - **Lead time is critical**
  - **Bad news doesn't get better with**



OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Improving Intelligence Integration in Acquisition

Intelligence Strategy, Programs and Resources

USD(I) coordinates intel for Acquisition/Requirements

- **Within Agencies**
- **Across Agencies**
- **National & Defense Intelligence**

How do you make the IC work for your Program?

Key Authoritative Documents:

- DoDD 5000.01, The Defense Acquisition System, 20030512, cert current 20071120
- DoDI 5000.02, Operation of the Defense Acquisition System, 20150107
- DoDD 5250.01, Management of Intelligence Mission Data in DoD Acquisition, 20130122
- CJCSI 5123.01, JROC Charter
- CJCSI 3170.01I, Joint Capabilities Integration and Development System, 20150123
- JCIDSM, Manual for the Operation of the JCIDS, 20150212
- DoDD 5240.02, Counterintelligence
- DoDM 5200.01, Information Security Program

Best Practice—Engage with intel early and often; at a minimum, meet milestone requirements

What's being done to improve the process?

- **Expanding focus of DODD 5250.01 from just Intel Mission Data to the Big 10—Threat plus 9 JCIDS Intelligence Supportability Categories:**
  - Intelligence Manpower Support
  - Intelligence Resource Support
  - Intelligence Planning and Operations Support
    - Planning and Direction
    - Collection (Includes SIGINT, HUMINT, MASINT, GEOINT support requirements)
    - Processing and Exploitation
    - Analysis and Production
    - Dissemination and Integration
    - Evaluation and Feedback
  - Targeting Support
  - Intelligence Mission Data Support
  - Warning Support
  - Space Intelligence Support
  - Counterintelligence Support
  - Intelligence Training Support
- **3 Key Focus areas: Threat, Intel Mission Data, Counterintelligence**

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Recognizing & Addressing IMD Demands

Intelligence Strategy, Programs and Resources

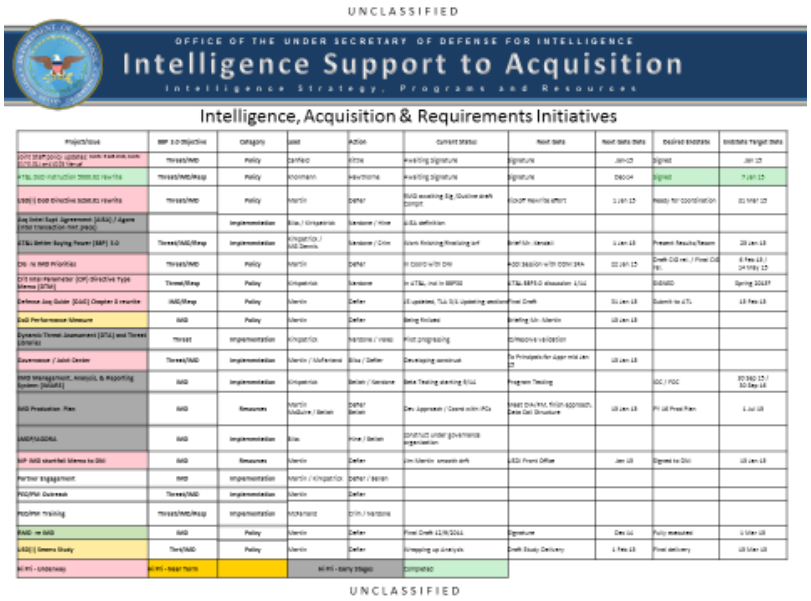
What's being done to improve the process? (continued)

- Coordination and alignment of DoD Efforts across Acquisition, Intelligence, and Requirements Communities

- Guiding Principles:
  - No new bureaucracy
  - Must leverage existing governance structures

Cross-domain efforts by Champion Governance

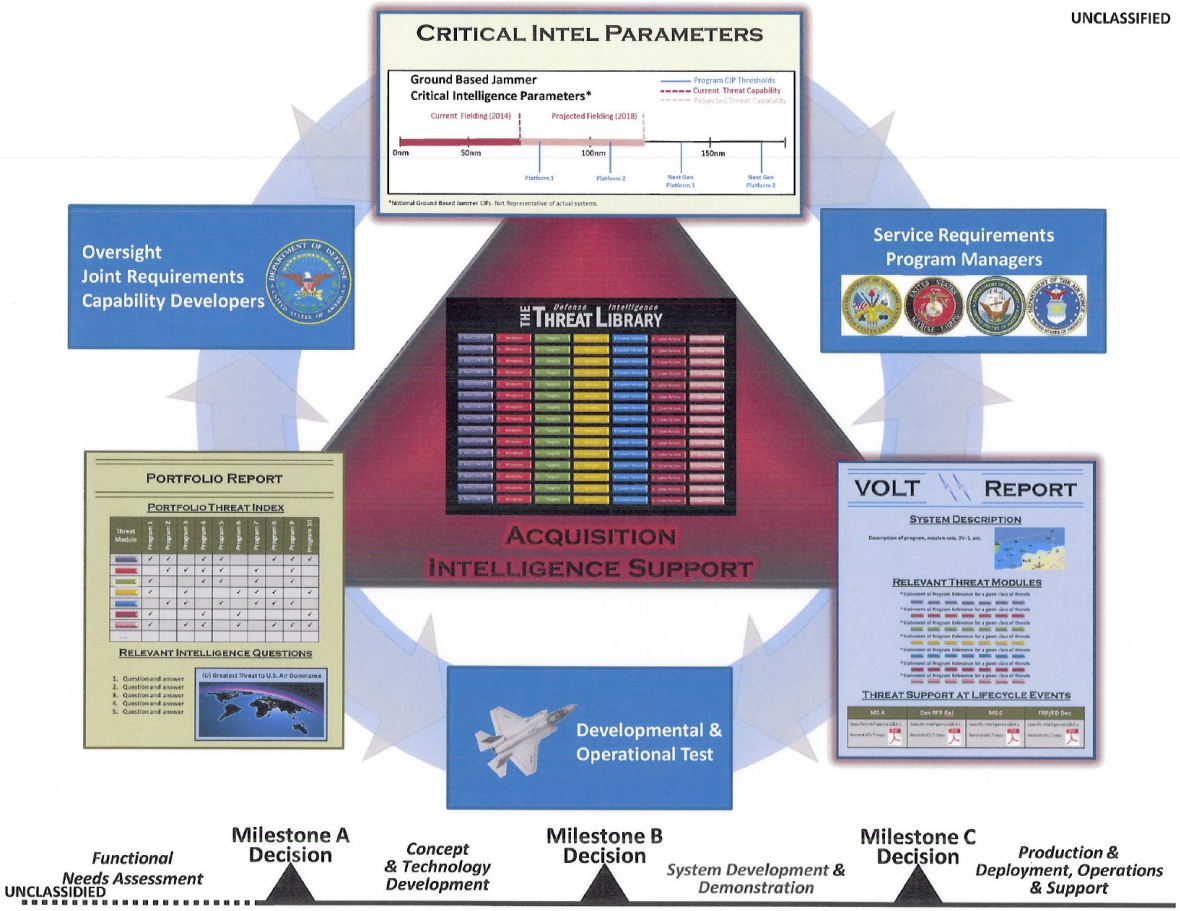
Intelligence	Acquisition	Requirements
• RMD	• BBP 3.0	• IRCO Certification
• CIG/IMD	• 5000.02	• JCIDS MANUAL
• DIAP efforts	• Agora (Market)	• JCIDS CJCSI
• 5250 Rewrite	• Acq Intel Spt Agmt (AISA)	
• CIP DTM	• Training	
• DAG Ch 8 rewrite		
• DoD Performance		


UNCLASSIFIED
OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
Intelligence Support to Acquisition
Intelligence Strategy, Programs and Resources
Intelligence, Acquisition & Requirements Initiatives
UNCLASSIFIED

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Improving Intelligence Integration in Acquisition

Intelligence Strategy, Programs and Resources



mportance of Threat to Development:

- **DIA coordination office – TLA-3**
- **Capabilities** are developed against the adversaries' capability
- **Threat(s)** can change during the development cycle
  - The enemy can develop new threats faster than we can develop new systems
  - Potential enemies access our media and exploit unprotected repositories of Defense related information
  - Potential adversaries have observed US capabilities in the field after more than a decade of hostilities
  - They know a great deal about the capabilities we employ and the major systems we are developing
- **Threat information** must be updated at CDD and CPD
- **Critical Intelligence Parameters (CIPs)** must be identified early

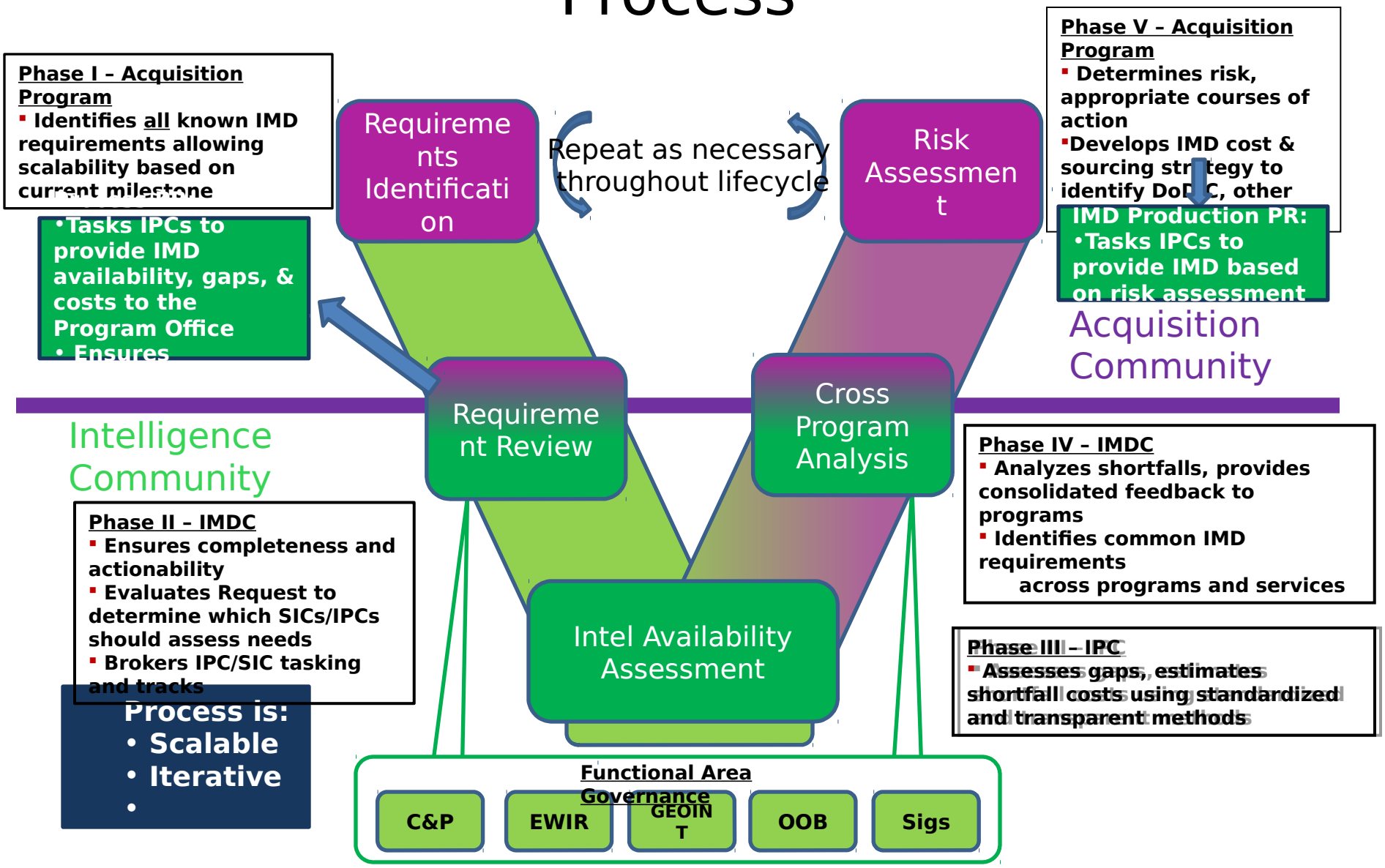
Critical Intelligence Parameters:

- **Definition:** CIPs are those key performance thresholds of foreign threat systems which, if exceeded, could compromise the mission effectiveness of the US system in development.
  - Identified in the System Threat Assessment Report (STAR); monitored by the IC; Breaches declared when applicable adversary threat advances observed
- **CIP Breach Process:**
  - Breach reviews use similar procedures to JROC/JCB tripwire reviews; intent is for Risk Mitigation Teams to address breach impacts on capability and associated programs
  - Strategic Program CIP Breach briefed to Force Application (FA) WG, FA FCB
    - CIP Breach did not present significant concern for sponsor or program
    - Review of the breach provided excellent opportunity to test and follow procedures
    - Mitigation Team participation included JS J8, DIA TLA-3, MSIC, NASIC, and JS J283
  - Incorporated throughout JCIDS Manual; OSD Directive-Type Memorandum (DTM) in coordination for incorporation in acquisition process
- **IRCO and DIA facilitating CIP Breach inclusion in FCB capability reviews**

Critical Intelligence Parameters

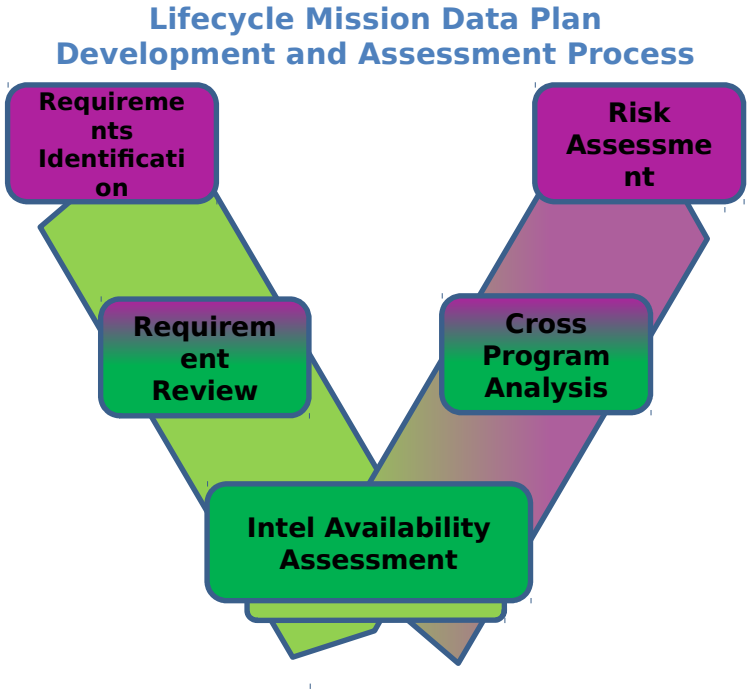
- Challenge
  - No DoD policy or guidance on CIPs existed
    - Only guidance in DIA Instruction related to STAR validation for large programs
  - No standardization across programs
    - Notification process not mandatory nor consistent
    - Programs self-police when threat exceeds parameters
- Status
  - CIP working group was established (JS, AT&L, USDI, DIA, Service Intel Centers)
  - New policy language (Directive-Type Memo) has been drafted, process defined
  - CJCSI 3170/JCIDS manual updated and made several improvements:
    - Identification of CIPs during CBAs when they are driving the capability requirements.
    - Threat Summary section of ICDs include identification of CIPs; CDDs & CPDs include summary of CIPs associated with KPPs, KSAs, and APAs.
    - CIPs as a component of Warning Support assessed in Intelligence Supportability content of CDDs and CPDs.
    - Staffing of Tripwires and CIP Breach Reviews.
    - Review of CIPs as part of Intelligence Certification
- Next Steps
  - BBP 3.0 action to provide formal DTM package to USD(AT&L) for approval then processing (usually 90-day process)

LMDP Development and Assessment Process


Phase I – Acquisition Program
▪ Identifies all known IMD requirements allowing scalability based on current milestone
•Tasks IPCs to provide IMD availability, gaps, & costs to the Program Office
• Ensures
Requirements Identification
Repeat as necessary throughout lifecycle
Risk Assessment
Phase V – Acquisition Program
▪ Determines risk, appropriate courses of action
▪Develops IMD cost & sourcing strategy to identify DoD C, other
IMD Production PR:
•Tasks IPCs to provide IMD based on risk assessment
Acquisition Community
Intelligence Community
Requirement Review
Cross Program Analysis
Phase II – IMDC
▪ Ensures completeness and actionability
▪ Evaluates Request to determine which SICs/IPCs should assess needs
▪ Brokers IPC/SIC tasking and tracks
Intel Availability Assessment
Phase IV – IMDC
▪ Analyzes shortfalls, provides consolidated feedback to programs
▪ Identifies common IMD requirements
across programs and services
Phase III – IPC
▪ Assesses gaps, estimates shortfall costs using standardized and transparent methods
Process is:
• Scalable
• Iterative
•
Functional Area Governance
C&P
EWIR
GEOINT
OOB
Sigs

Coming Improvements: IMARS System

- The IMD Management, Analysis and Reporting System (IMARS) is a tool to facilitate the identification, assessment and analysis of IMD requirements
- IMARS saves IMD requirements and requirements, making it easier to update the LMDP throughout the program lifecycle
- IMARS v1.2 (IOC Version) expected completion ~ Sep 15
  - IMD supportability assessment & cross program analysis capabilities
- IMARS v2.0 (FOC Version) complete ~Sep 16
  - Adds time-phased IMD requirements



Resource Management Decision Directs Three Actions:

- Joint Staff–Conduct a Capabilities Based Assessment of IMD production capability requirements, linking IMD to KPPs
- USD(I)–Work with ODNI and Mil Depts to discretely identify/ track resources to satisfy IMD production, develop business process for appropriate allocations
- USD(AT&L)—Develop a Governance Structure – identify, prioritize and address resourcing and prioritization of cradle to grave IMD requirements

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Improving Intelligence Integration in Acquisition

Intelligence Strategy, Programs and Resources

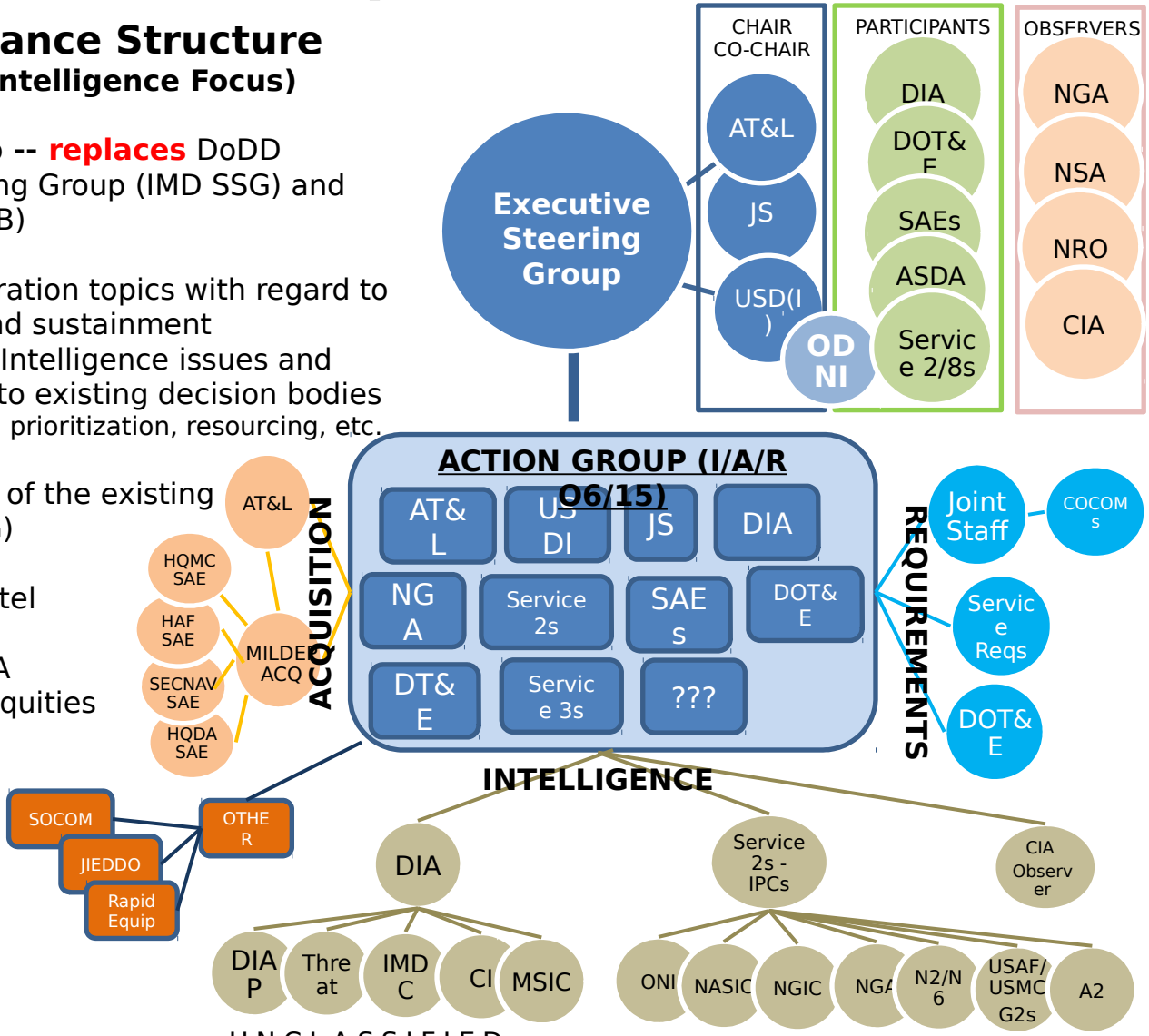
Conceptual Governance Structure
(IMD – THREAT – Counterintelligence Focus)

Executive Steering Group -- replaces DoDD 5250.01's IMD Senior Steering Group (IMD SSG) and IMD Oversight Board (IMD OB)

- Address Intelligence integration topics with regard to capability development and sustainment
- Prioritize DoD Acq related Intelligence issues and submits for consideration to existing decision bodies
  - Risk Analysis, IMD POA, prioritization, resourcing, etc.

Action Group -- evolution of the existing IMD Working Group (IMD WG)

- Coordinate/Synchronize Intel
- Integration issues
- Manage/facilitate AISA/CPA
- Clearing house Intel/Acq equities
- Service 2s, 3s and SAEs
- involvement critical
- Training/Outreach



OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

IMD Shortfall Deep Dive

Intelligence Strategy, Programs and Resources

- Data exists for F-35 IMD requirements/shortfalls for Blocks 2/3, AORs 1-4, FY15; *No update will be completed in time for the FY 2017 Issue Paper*

- IMDC has requirements/gaps assessed for 9 programs, using CAPE approved costing methodology; up to 8 additional programs may be captured

Assessed LMDPs:

PAC-3 (Army)
IFPC (Army)
AMDR (2013 & 2014) (Navy)
SDB-II (USAF)
F-35 (2013 & 2014) (Joint)
RQ-4 Global Hawk (USAF)
RQ-21 Blackjack (USMC)

Identified for RMD:

B2 DMS (USAF)
EPAWSS(USAF)
NGJ (Navy)
GROWLER (Navy)
LCS Mission Module (Navy)
CREW (USMC)
DCGS-A (Army)
IGSSRC (Army)

The IMD shortfall is Department wide

Counterintelligence Challenges:

- **IRCO observations regarding CI requirements and supportability** in capability development
  - **Inconsistent and insufficient identification of CI support** needed to mitigate foreign threat vulnerabilities and provide program protection
    - **Lack of supporting threat assessments and plans** – Multi-Discipline CI Threat Assessment, Technology Transfer Risk Assessment, Supply Chain Threat Assessment, CI Support Plan – augment the Program Protection Plan (PPP)
    - **Insufficient Sponsor understanding of CI** support issues
    - **Supporting assessments and plans** are primarily acquisition requirements; however, **serve to inform CI support category requirements**
  - **Possible capacity issues** across the Intelligence Community (IC) to process threat assessments
  - Assessment complements the USD(I) and AT&L Joint Acquisition Protection Exploitation Cell (JAPEC) task to protect against loss of technical information
- **Sponsor / PM should initiate CI-related vulnerability assessments early in development**
  - Take into account shared (foreign partner) production and Supply Chain Risk

Take Away:

- Multiple initiatives across Acquisition, Intelligence, and Requirements Communities to improve processes and responsiveness
- Key focus areas: Threat, Intel Mission Data, and Counterintelligence
- Automated Intelligence Support Agreement under development:
  - Documents program intelligence requirements and shared expectations
  - Under development at this time; expected out in FY 2016
- Best Practice: Early Engagement and Regular Dialogue

Backup Slides

New CIP Process